IN THE CLAIMS:

Please amend the claims as follows. This listing of the claims will replace all prior versions of the claims in the application.

1. – 104. (Cancelled)

105. (Currently Amended) A computer-implemented method comprising:

selecting an active program on a computer system as code under investigation, wherein at least some of the code associated with the selected active program is running in kernel mode; and

executing malicious code detection code (MCDC) on the computer system, wherein the MCDC includes a first and a second plurality of detection routines, wherein said executing includes:

applying each of the first plurality of detection routines to the code under investigation to obtain a corresponding one of a first plurality of results;[[,]] ~~wherein said applying includes associating weights to the code under investigation in response to detections of a valid program or malicious code; and~~

weighting each of the first plurality of results to obtain a first score indicative of whether the code under investigation is valid code;

applying each of the second plurality of detection routines to the code under investigation to obtain a corresponding one of a second plurality of results;

weighting each of the second plurality of results to obtain a second score indicative of whether the code under investigation is malicious code; and

using the first and second scores to determine[[ing] whether the code under investigation is ~~a valid program or~~ malicious code ~~as a function of the weights associated by the detection routines~~.

106. (Previously Presented) The method of claim 105, wherein the code under investigation has access to other active programs executing on the computer system.

107. (Currently Amended) The method of claim 105, further comprising:

selecting one or more additional active programs as code under investigation; and

executing said MCDC with respect to said selected code under investigation.

108. (Cancelled)

109. (Previously Presented) The method of claim 105, wherein the malicious code includes remote control software.

110. (Previously Presented) The method of claim 105, wherein the malicious code includes a keystroke logger.

111. (Previously Presented) The method of claim 105, wherein the malicious code includes spyware.

112. (Previously Presented) The method of claim 105, wherein the malicious code includes a worm.

113. (Previously Presented) The method of claim 105, wherein the malicious code includes a virus.

114. (Previously Presented) The method of claim 105, wherein the malicious code includes monitoring software.

115. (Currently Amended) A computer-implemented method comprising:

selecting ~~a program~~ code currently running on a computer system as code under investigation, wherein said ~~program~~ code is running in a manner that permits infection of said computer system; and

executing malicious code detection code (MCDC) on the computer system, wherein the MCDC includes a first and a second plurality of detection routines, wherein said executing includes:

applying each of the first plurality of detection routines to the code under investigation to obtain a corresponding one of a first plurality of results ~~,~~

~~wherein said applying includes associating weights to the code under investigation in response to detections of a valid program or malicious code~~; ~~and~~

weighting each of the first plurality of results to obtain a first score indicative of whether the code under investigation is valid code;

applying each of the second plurality of detection routines to the code under investigation to obtain a corresponding one of a second plurality of results;

weighting each of the second plurality of results to obtain a second score indicative of whether the code under investigation is malicious code; and

using the first and second scores to determine[[ing] whether the code under investigation is ~~a valid program or~~ malicious code ~~as a function of the weights associated by the detection routines~~.

116. (Currently Amended) The method of claim 115, wherein the code under investigation has access to other active ~~programs~~ code executing on the computer system.

117. (Currently Amended) The method of claim 115,wherein at least some of the code associated with the selected active ~~program~~ code is running in kernel mode.

118. (Currently Amended) The method of claim 115, further comprising:

selecting ~~one or more~~ additional active code ~~programs~~ as code under investigation; and

executing said MCDC with respect to said selected code under investigation.

119-126. (Cancelled)

127. (Currently Amended) A computer system comprising:

a processor; and

a memory storing program instructions executable by the processor to:

select a program currently running on a computer system as code under investigation, wherein said program is running in a manner that permits infection of said computer system; and

execute malicious code detection code (MCDC) on the computer system, wherein the MCDC includes a first and a second plurality of detection routines, including:

applying each of the first plurality of detection routines to the code under investigation to obtain a corresponding one of a first plurality of results ~~, wherein said applying includes associating weights to the code under investigation in response to detections of a valid program or malicious code~~; ~~and~~

weighting each of the first plurality of results to obtain a first score indicative of whether the code under investigation is valid code;

applying each of the second plurality of detection routines to the code under investigation to obtain a corresponding one of a second plurality of results;

weighting each of the second plurality of results to obtain a second score indicative of whether the code under investigation is malicious code; and

using the first and second scores to determine[[ing] whether the code under investigation is ~~a valid program or~~ malicious code ~~as a function of the weights associated by the detection routines~~.

128. (Currently Amended) A computer-readable memory medium, including program instructions that are computer executable to:

select a program currently running on a computer system as code under investigation, wherein said program is running in a manner that permits infection of said computer system; and

execute malicious code detection code (MCDC) on the computer system, wherein the MCDC includes a first and a second plurality of detection routines, including:

applying each of the first plurality of detection routines to the code under investigation to obtain a corresponding one of a first plurality of results;~~, wherein said applying includes associating weights to the code under investigation in response to detections of a valid program or malicious code; and~~

weighting each of the first plurality of results to obtain a first score indicative of whether the code under investigation is valid code;

applying each of the second plurality of detection routines to the code under investigation to obtain a corresponding one of a second plurality of results;

weighting each of the second plurality of results to obtain a second score indicative of whether the code under investigation is malicious code; and

using the first and second scores to determine[[ing] whether the code under investigation is ~~a valid program or~~ malicious code ~~as a function of the weights associated by the detection routines~~.

129. (New) The method of claim 105, further comprising:

determining from the first and second scores that the code under investigation is malicious code.

130. (New) The method of claim 129, wherein the malicious code does not have a known signature.

131. (New) The method of claim 105, wherein a signature associated with the code under investigation is not used by the first plurality of detection routines.

132. (New) The method of claim 131, wherein a signature associated with the code under investigation is not used by the second plurality of detection routines.

133. (New) The method of claim 105, wherein the first and second plurality of detection routines are not specific to the code under investigation.

134. (New) The method of claim 129, wherein the determination that the code under investigation is malicious code is based on the first score not exceeding a valid code threshold value and the second score exceeding a malicious code threshold value.

135. (New) The method of claim 105, further comprising:

determining from the first and second scores that the code under investigation is valid code.

136. (New) The method of claim 135, wherein the determination that the code under investigation is valid code is based on the first score exceeding a valid code threshold value.

137. (New) The method of claim 105, further comprising:

determining from the first and second scores that the code under investigation is suspicious code, wherein suspicious code has not been determined to be either valid or malicious code.

138. (New) The method of claim 137, wherein the code under investigation is determined to be suspicious code based on the first and second scores being similar.

139. (New) The system of claim 127, further comprising program instructions executable by the processor to:

determine from the first and second scores that the code under investigation is malicious code.

140. (New) The system of claim 139, wherein the malicious code does not have a known signature.

141. (New) The system of claim 139, wherein the determination that the code under investigation is malicious code is based on the first score not exceeding a valid code threshold value and the second score exceeding a malicious code threshold value.

142. (New) The system of claim 127, further comprising program instructions executable by the processor to:

determine from the first and second scores that the code under investigation is valid code.

143. (New) The system of claim 142, wherein the determination that the code under investigation is valid code is based on the first score exceeding a valid code threshold value.

144. (New) The system of claim 127, further comprising program instructions executable by the processor to:

determine from the first and second scores that the code under investigation is suspicious code.

145. (New) The memory medium of claim 128, further comprising program instructions executable to:

determine from the first and second scores that the code under investigation is malicious code.

146. (New) The memory medium of claim 145, wherein the malicious code does not have a known signature.

146. (New) The memory medium of claim 145, wherein the determination that the code under investigation is malicious code is based on the first score not exceeding a valid code threshold value and the second score exceeding a malicious code threshold value.

147. (New) The memory medium of claim 128, further comprising program instructions executable to:

determine from the first and second scores that the code under investigation is valid code.

148. (New) The memory medium of claim 147, wherein the determination that the code under investigation is valid code is based on the first score exceeding a valid code threshold value.

149. (New) The memory medium of claim 128, further comprising program instructions executable to:

determine from the first and second scores that the code under investigation is suspicious code.